A Guide to Cyber Crime and Online Safety

BLOCK THE WEB MONSTERS

www.westyorkshire.police.uk/BlockTheWebMonsters

Office of the Police & Crime Commissioner West Yorkshire

WEST YORKSHIRE POLICE

This guide has been designed to give you and your family basic crime prevention tips for when you are online. The aim is to equip you with the necessary advice and tips that may reduce the likelihood of you or one of your family members becoming a victim.

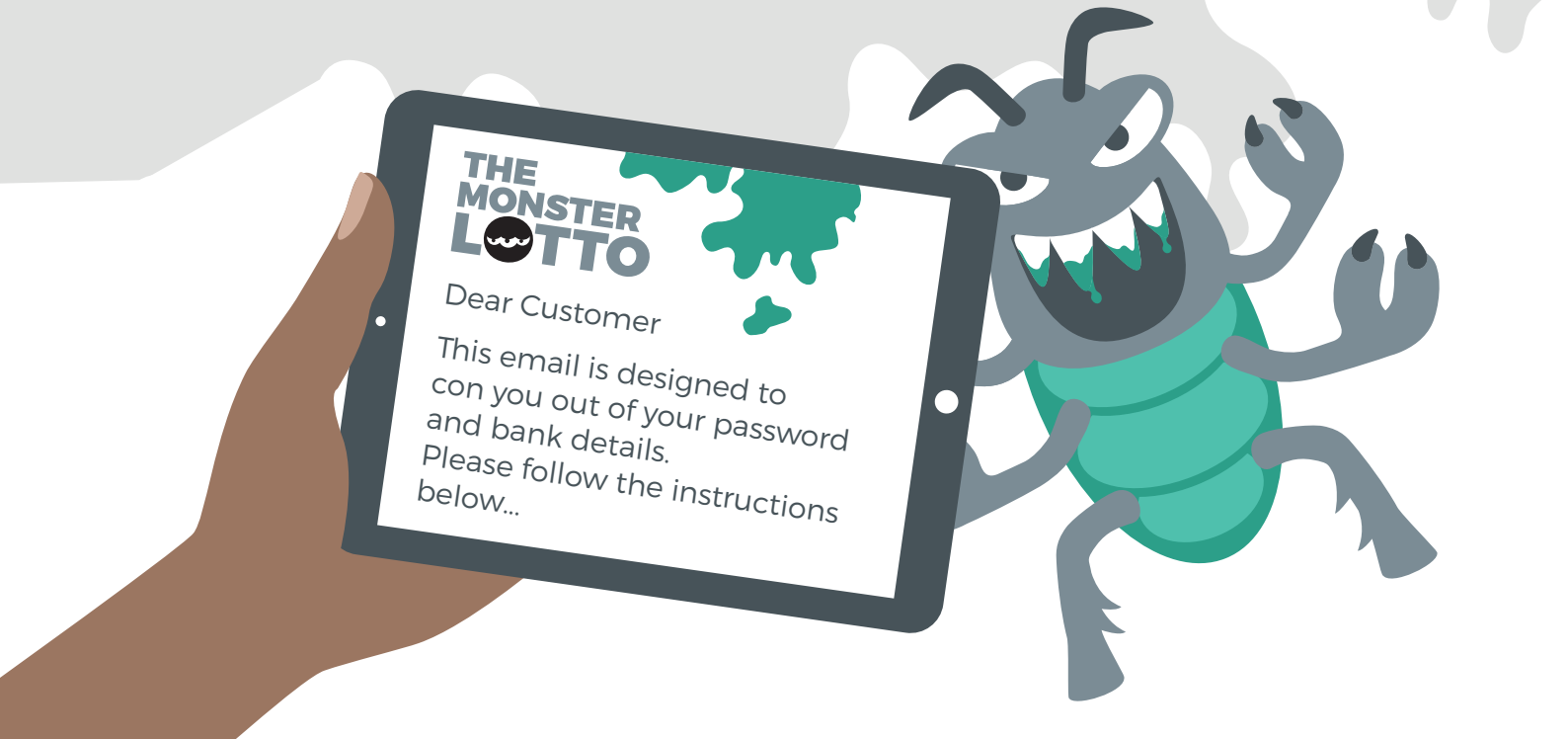
West Yorkshire Police is only one of a handful of forces across the country with a dedicated Cyber Unit. The Unit is looking to advise you about the dangers of the crime and the devastating impact it can have on people's lives.

"The computer is rapidly becoming the new crowbar and anyone who has a desktop computer, laptop, tablet or mobile device / phone could be at risk of being a victim"

DCI Vanessa Smith - Regional Cyber Crime Unit

Contents

What is Cyber Crime?	1
Online Fraud / Scams	2
Phishing	2
Pharming	3
Spam Emails	4
Online Shopping	5
Online Banking	6
Identity Theft	7
Grooming / Child Sexual Exploitation	8
What to do?	9
Spot it early	9
Other forms of Online Grooming	10
Advice for Parents	11
Social Media Safety	12
General Safety Tips	12
Sexting	13
Sexting - How to combat	14
Online Bullying	15
Pathways into Cyber Crime	16 - 17
Smartphone and Tablet Safety	18
Glossary	19
More advice online	20


THE MONSTER LOTTO
Dear Customer
This email is designed to con you out of your password and bank details.
Please follow the instructions below...

What is Cyber Crime?

It can be argued that the internet is a technology that has enhanced our lives. It allows us to communicate with people around the world, search for information at a click of a button and shop without having to leave your house.

Equally it can also be said that the internet has generated many risks and threats. It has helped to increase the scale and reach of traditional crimes as well as introducing new types of crimes where computer systems are the target.

The term cyber crime refers to a variety of crimes carried out online using the internet through computers, laptops, tablets, smart TVs, games consoles and smart phones.

Cyber crime falls into two different categories:

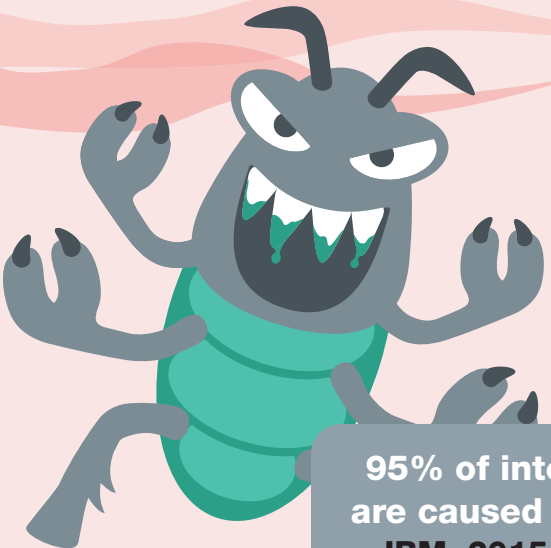
- **Cyber-enabled crime** - traditional crimes which can be increased in scale or reach by the use of the internet. These can include theft, harassment, fraud, identity theft, selling stolen goods, drug dealing etc

- **Cyber-dependent crime** - online crimes where a digital system is the target. These include attacks on computer systems to disrupt IT infrastructures, such as; unauthorised access (hacking), malicious software programming (malware) or a distributed denial of service attack (DDos)

Cyber crime impacts upon all areas of our society. It can affect people in different ways leaving victims feeling worried and scared by what has happened.

Due to the nature of cyber crime, anyone can be a victim. It might be a young person who is bullied online or an older person who has been scammed out of money.

It's vitally important to protect yourself from these threats and safeguard your online personal security.



95% of internal breaches are caused by human error IBM, 2015 cyber security intelligence index

Online Fraud / Scams

Online fraud covers a variety of incidents - including online banking, identity theft and online shopping to name just a few. Users often forget that they are not dealing face to face with someone and believe what they see to be true. Many may not apply the same sort of caution you take when dealing with someone face to face.

Phishing

Phishing emails are intended to deceive you into thinking they are a communication from a legitimate organisation, such as your bank or one of your online accounts. The website will look genuine and can be a clone of a genuine site. Once you input your data, the website then captures your details and can be used fraudulently.

What should I do?

- ✔ Do not click on links from suspicious emails
- ✔ Most banks and organisations will never ask you for your password or PIN numbers
- ✔ If in doubt, telephone the alleged source of the email to verify if it is genuine
- ✔ Never enter your personal information on a website unless you are sure it is legitimate
- ✔ Always check the web address of the web page you are visiting and ensure it is the official website
- ✔ For extra precaution it is advisable to type the address in manually or navigate to it through other ways to ensure it is a genuine website
- ✔ Never reply to these emails - you may then be added to a 'victims' list and receive more emails of a similar kind

What to look out for

Amazon Update <AmazonUpdate@efficaciouscrbays.xyz
to me
Does the email address look genuine?
Why is this message in Spam? It's similar to messages that were detected by our spam filters. Learn more
amazon.com Prime
Genuine companies will address you by your name
The Amazon Marketplace
-----SHOPPER/MEMBER:4726
-----DATE-OF-NOTICE: 12/22/2015
Is the link genuine? Always hover over link to check
Hello Shopper: @gmail.com! To show you how much we
with us and to celebrate the continued success of our Prime membersh
with-$100 in shopping points that can be used on any item on our online shopping site! (this includes any marketplace vendors)
In order to use this-$100 reward, simply go below to get your-coupon-card and then just use it during checkout on your next purchase. That's all there is to it!
Please visit-here now to get your reward
Will genuine companies choose this kind of wording?
***DON'T WAIT! The Link Above Expires on 12/28!

Pharming

Pharming is another method hackers use to manipulate users on the Internet. While phishing attempts to capture personal information by getting users to visit a bogus website, pharming redirects users to false websites without them even knowing.

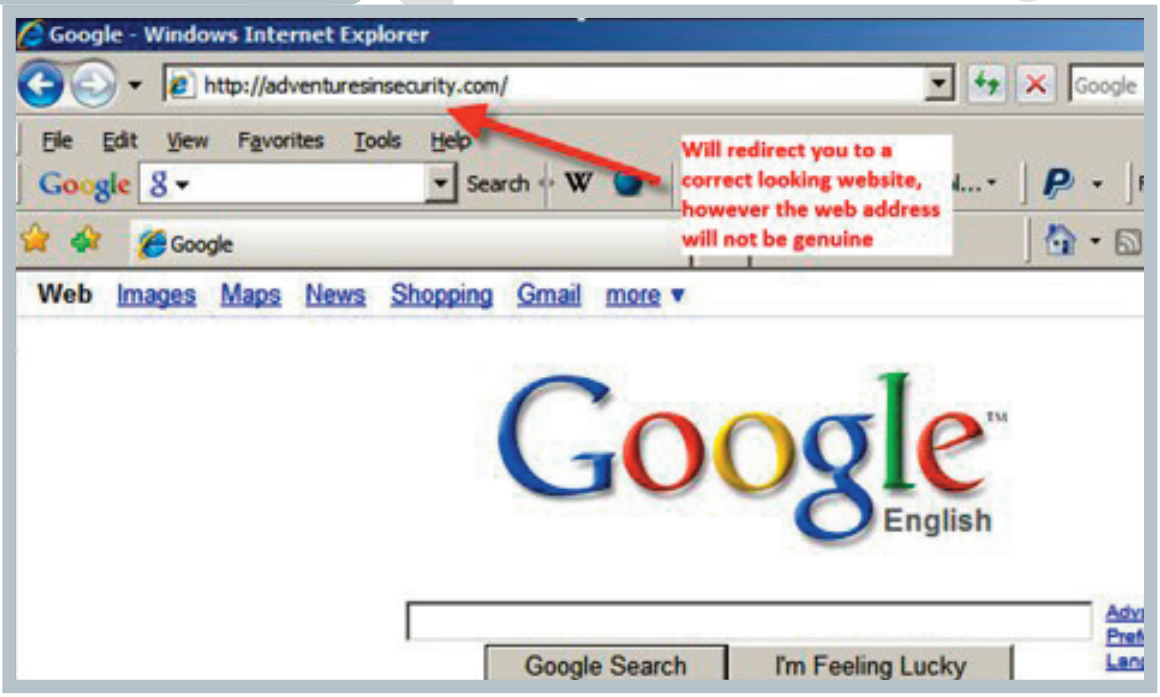
One way that pharming takes place is via an email virus that infects the computer. It redirects the IP address of a genuine website to another similar looking website determined by the hacker.

While pharming is not as common as phishing scams are, it can affect many more people at once.

What should I do?

- ✔ Run an antivirus program
- ✔ Restart your computer to reset your DNS (website) entries
- ✔ If the website still looks strange, contact your Internet Service Provider (ISP) and let them know their DNS server may have been pharmed
- ✔ Ensure that once the page has loaded, that the URL (website address) is spelt correctly and hasn't redirected to a slightly different spelling, e.g. with an additional letter or a letter swapped around

Example of Pharming


Google - Windows Internet Explorer
http://adventuresinsecurity.com/
File Edit View Favorites Tools Help
Will redirect you to a correct looking website, however the web address will not be genuine
Web Images Maps News Shopping Gmail more
Google
English
Google Search
I'm Feeling Lucky

Spam / Scam Emails

Unwanted emails typically result from having visited a website or having entered your personal email.

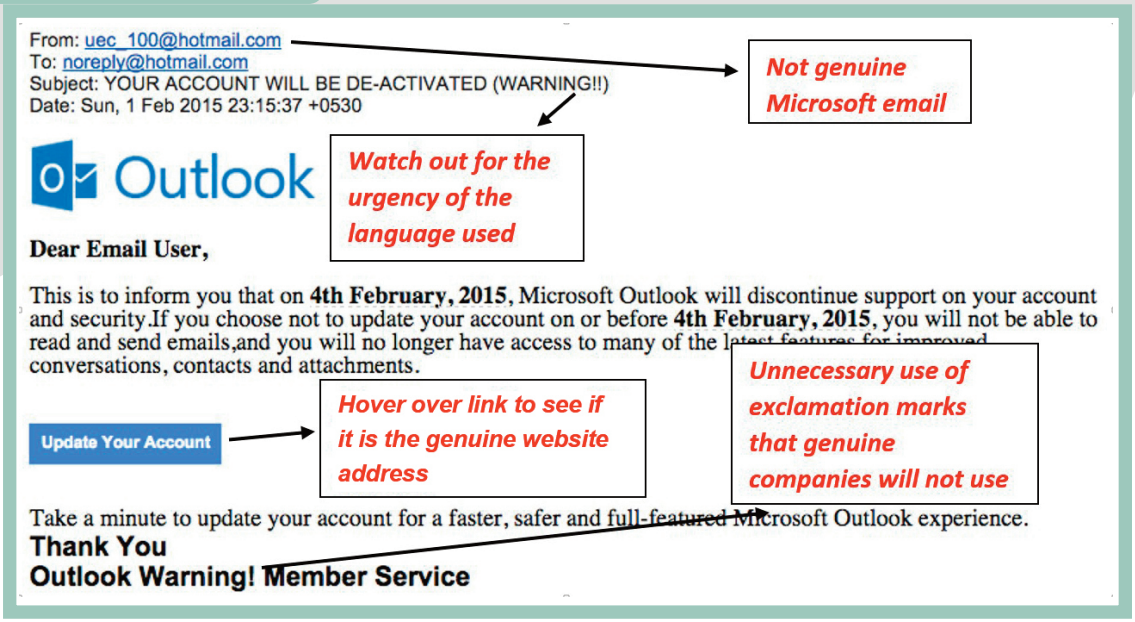
This could include “Get rich quick” schemes or advertising of goods or services. Scammers may try to get your attention by saying the offer is “urgent”, “just for you”, or make claims which seem too good to be true.

These emails may even come across as an urgent message and may appear to originate from an enforcement or other legitimate agency, i.e. “Warning from Police.”

What should I do?

- ✔ Do not open emails you suspect may be scams
- ✔ Do not respond to emails from unknown sources
- ✔ If in doubt, contact the person or organisation to verify if it is genuine
- ✔ Do not open attachments on dodgy emails, they may install malicious software on your computer
- ✔ Do not click on any links within the email. These can contain viruses or take you to websites containing inappropriate material
- ✔ Ensure that spam filters are activated on your email account

What to look out for

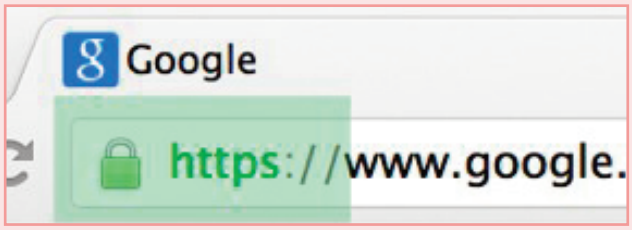

From: uec_100@hotmail.com
To: noreply@hotmail.com
Subject: YOUR ACCOUNT WILL BE DE-ACTIVATED (WARNING!!)
Date: Sun, 1 Feb 2015 23:15:37 +0530
Not genuine Microsoft email
Outlook
Watch out for the urgency of the language used
Dear Email User,
This is to inform you that on 4th February, 2015, Microsoft Outlook will discontinue support on your account and security.If you choose not to update your account on or before 4th February, 2015, you will not be able to read and send emails,and you will no longer have access to many of the latest features for improved conversations, contacts and attachments.
Update Your Account
Hover over link to see if it is the genuine website address
Unnecessary use of exclamation marks that genuine companies will not use
Take a minute to update your account for a faster, safer and full-featured Microsoft Outlook experience.
Thank You
Outlook Warning! Member Service

Safe Online Shopping

Shopping online can often save time and effort but there are risks too.

What should I do?

- ✔ Make sure the retailer is reputable, research them online and make sure they have an address and phone number
- ✔ Look out for secure "https" links in the address of the website to ensure the site is secure in its payment



- ✔ Look for a padlock symbol when making purchases, this confirms that the site encrypts your data when it is sent
- ✔ Use a secure internet connection when online shopping, avoid using public Wi-Fi
- ✔ Paying online by credit card can offer greater protection than other payment methods
- ✔ When making a payment, use a secure payment site such as PayPal
- ✔ Try to use different passwords for different websites - sharing passwords can be very risky
- ✔ Fake scam versions of corporate sites may be set up that look almost identical to the original site - yet may be completely fake. Always check the web address of the page and ensure it is the official website
- ✔ Always check your credit card and bank statements to make sure that the correct amount has been debited
- ✔ Keep receipts

Online Banking

The average customer of certain UK banks view their finances on their phone more than once a day – much of this balance checking and payment making is done while people watch TV
British Bankers' Association, 2016

Online banking can be very convenient, where it can enable you to complete many of your banking tasks without the hassle of waiting in queues or needing to book an appointment.

However, there are risks associated to online banking too. Be aware that cyber thieves can target accounts you access via phishing emails and password theft, which may put you at risk of fraud.

So always remember to protect yourself.

What should I do?

- ✔ Use strong passwords
- ✔ Keep passwords and personal details private to stop criminals accessing your account. Banks will never ask you to reveal your full password on the phone or by email
- ✔ Be aware of who can see your screen and make sure you log out properly
- ✔ Use a secure internet connection when online banking, avoid using public Wi-Fi
- ✔ Ensure you have effective and updated antivirus / antispyware software and firewall running before you log in to your bank account
- ✔ Keep your software up to date
- ✔ Check your account often - will help you to detect any breaches or anomalies

The average branch in the high street deals with only 71 customer visits a day – a 32% decline since 2011 – as consumers switch to online methods of managing money
British Bankers' Association, 2016

Identity Theft

Identity theft is a form of fraud that occurs when a dishonest person gets hold of your personal information and uses it to their advantage to steal directly from you, or commit a crime in your name.

Identity thieves are increasingly using personal information displayed on social media sites to access the information that they need.

69% of people in Yorkshire region said their top concern is identity theft
Get Safe Online and NFIB, 2016

What should I do?

- ✔ Do not divulge personal information or post it on social media sites in response to emails, calls and texts
- ✔ Ensure what you post online does not contain any information that may be used against you in committing fraud
- ✔ Take precautions when performing online transactions, be sure the site is secure and the company is known to be reputable
- ✔ Carefully check your monthly statements for any unauthorised or missing transactions
- ✔ File sensitive documents securely, don't just throw them in the bin, shred them before disposing safely
- ✔ Consider using a credit reference agency, such as Experian, and check it regularly for unusual or unexpected changes

✔ **Passwords:**

1. Do not share your PIN or Passwords
2. Choose a strong password with 8 characters or more
3. Do not reuse your passwords across multiple sites
4. Do not use passwords which could be easily guessed or obtained through social media
5. Use two factor authentication whenever possible. This requires you to enter a PIN, usually sent to your mobile phone when you log in to assist in proving your identity

Examples of difficulty	
Password	**Time to crack**
1994	Almost instantly
aFv7!	0.677 seconds
8H_p(8	52 seconds
@t}9Nra	5 hours
93z<D2SY	5 days
f!*E7"BUx	5 years
}[vBbaX5=Z	526 years
8_3aM=:4#RM	50,000 years
R6tvSnn?:7@(	4 million years

43% of people in the Yorkshire region use the same password for multiple online accounts
Get Safe Online and NFIB, 2016

Online Grooming / Child Sexual Exploitation

Grooming is when someone builds an emotional connection with children to gain their trust for the purposes of sexual abuse, sexual exploitation or trafficking.

Children and young people can be groomed online or face to face, by a stranger or by someone they know.

Groomers will use a variety of ways to get what they want. They will hide their true intentions, they may:

- Pretend to be someone they are not, i.e. say they are the same age
- Offer advice or understanding
- Give the child attention
- Tell children what they want to hear

Online sexual exploitation can lead to young people being persuaded or forced to:

- Post sexually explicit images of themselves
- Take part in sexual activities via a webcam or smartphone
- Have sexual conversations by text or online
- To meet in person

There were over 11,000 counselling sessions with young people who talked to Childline about online issues last year
NSPCC, 2016

Grooming - Online Dating

It is also worth mentioning that adults can be groomed as well, especially through online dating sites.

Additionally a lot of users of these sites can also be victims of romance scams.

Therefore when using such sites remember to:

Take your time - Sometimes when you're excited about someone, your instincts and judgement may become confused. Always remember to take care and think about the situation at hand.

Report suspect behaviour - If something doesn't feel right, trust your instincts and report the behaviour.

What to do if you think you're being groomed?

Ask the person to stop - You might want to deal with the situation yourself. You can ask the person to stop - tell them you don't feel comfortable with what is happening.

Tell an adult you trust - It is extremely important to tell an adult you trust. Telling someone may seem embarrassing or hard to do at first but the sooner you talk the better.

Report it - You can report an adult or stranger if they've sent you a sexual message/image, asked you to send them a sexual message/image, sent anything that makes you feel uncomfortable or asked you to meet up with them.

This can be via -

- Child Exploitation and Online Protection Centre (CEOP) **https://www.ceop.police.uk/Ceop-Report/**

- The Internet Watch Foundation (IWF), they try to remove any illegal images posted online - **https://www.iwf.org.uk/**

- The website 'Childline' offers step by step instructions on how to report on different social media outlets **https://www.childline.org.uk/info-advice/bullying-abuse-safety/online-mobile-safety/sexting/**

Spot it Early

Online predators are hard to identify at first; they may seem like a normal person just like anyone else. However behind a screen their intentions are unknown. They will use fake accounts with fake profile pictures and fake information which makes it really difficult to tell who you are talking to and what age they are.

Below are some methods groomers may use which can help in spotting them early:

- **'Nice guy' approach** - will have conversations with you in a non-threatening way
- **Private conversations** - divert conversations where it is one on one
- **Inquisitive** - will ask a lot of questions
- **Agreement** - will agree with you to gain your trust
- **Try to make you feel special** - constantly tell you how important you are to them
- **Will want to see you in a vulnerable state** - quotes like, "What's wrong?" or "Tell me what's bothering you"
- **Mind games** - will try to turn you against other people
- **Gifts** - may offer you gifts, do not accept them
- **Request pictures / videos** - may ask you for pictures / videos, refuse it
- **Pressuring** - may pressure you into meeting in person
- **Sense of Normality** - try to make you think what they're doing is normal

Other Forms of Online Grooming

Online grooming can also take other forms including:

Online Radicalisation

Extremist groups and / or individuals are using social media to radicalise individuals, especially young people. They tend to target groups of people who can be easily led because of their state of mind, their upbringing or their experiences.

They also target individuals who express concerns over a lack of 'identity' and 'belonging' in communities. Extremists will exploit this in an attempt to lure a victim out of 'isolation'.

Sometimes individuals may actively search for online radical content, in doing so extremist individuals can manipulate to their own advantage and use this interest to initiate contact.

Signs indicating an individual may be at risk:

- **Isolation** - from family and friends
- **Secretive** - especially around internet use
- **Attitude** - intolerant and single minded attitude towards others
- **Sympathy** - with violence and extremist viewpoints
- **Anger** - increased levels of anger

Criminal Gang / Drug Dealing Involvement

There are cases around the country where children are being groomed to join criminal gangs for drug dealing. Children as young as 12 are being used as mules.

The use of children by criminal gangs is seen as beneficial and profitable primarily for the reason that gang members can exert their control. Groomers also use material gifts or promise of money in a bid to entice them.

Although online methods of grooming may not always be used for this, a report by the NCA in 2016 outlines that young people are targeted through homeless hostels and social media.

How to Combat?

Report to -

- ✔ Local Police
- ✔ Child Exploitation and Online Protection Centre (CEOP)

Be wary of -

- ✔ **Behaviour** - change in behaviour, mood or physical appearance
- ✔ **Violence** - look out for bruises or signs of physical violence
- ✔ **Goods** - be wary of large amounts of money or expensive goods in their possession

Advice for Parents

There are many signs, symptoms and effects of online child sexual abuse. If you are concerned about your child or a child you know then spotting the signs early can be a great preventative measure.

Signs, symptons and effects

- Spending large amounts of time online, especially at night
- Secretive about who they're talking to and what they're doing
- Having lots of new contact numbers, texts and phone calls
- Finding pornography on device they are using
- Unexplained appearance of gifts
- Turning the computer monitor off or quickly changing the screen
- Becoming withdrawn from family and friends
- Using an online account belonging to someone else
- Edgy new behavior, dress, language, makeup, or appearance
- Truancy in school
- Experimenting in drugs, smoking and alcohol

If doubts arise about your child, start a conversation:

- Find a good time and place
- Think about what to say and how to introduce subject
- Explain to them why you are worried
- Let them talk, listen more
- Be loving and supportive

Report

If you see or start to notice some of these signs, take action immediately. You can do this by reporting anything inappropriate to the CEOP (Child Exploitation and Online Protection) page.

Click on the image to make a report to CEOP

You can also ring **Childline on 0800 1111**

70% of parents look to their child's school for advice about internet safety

Cybersafe Opinion Leader Report, Sept 2013

Social Media Safety

One of the most popular activities on the internet is joining social networking sites. These sites provide opportunity to conduct many types of activities including communication and sharing.

Below are some tips for safe social networking that will help to keep you safe across all social media outlets including Facebook, Twitter, Snapchat and Instagram.

Keep Control

- ✔ Keep control over the information you post
- ✔ Limit the information about yourself. Don't post personal information like your full name, address, phone number, or any kind of financial or personal information Criminals could obtain this information to help them commit fraud against you
- ✔ Be cautious about information that can be used to identify you or locate you offline
- ✔ Do you really need location settings turned on? Sharing your location means that people can find out where you frequent or where you are

Privacy

- ✔ Use privacy controls to restrict access to your page
- ✔ Check your privacy settings and ensure that they are right for you. If your privacy settings are set to public, anyone can usually view your posts whether you are friends or not. This might also include things like where you are, and who you are with
- ✔ Try and keep your privacy settings high to ensure you are only sharing with people you know

Don't talk to strangers

In 'real life' would you let your child talk to strangers?
Would you go around showing photos of your family to strangers walking past?

If it is not ok offline then why is it ok online?

- ✔ Don't accept friend requests from people that you do not know
- ✔ Never engage a stranger in conversation online
- ✔ Avoid using websites that let you chat to people anonymously, you never know who you are really talking to
- ✔ Do not use video chat services with people that you do not know. They might encourage you to do things that you would not normally do, such as expose yourself

9% of victims in the Yorkshire region had their email or social media accounts hacked
Get Safe Online and NFIB, 2016

‘Social Media Enabled’ Crime

As mentioned, social media is one of the most popular activities on the internet. Within it, it can create a wide variety of ‘social media enabled’ crime.

Sexting

“Sexting” is a term used to describe the sharing of intimate images or video with another person. They can be sent using any device that allows you to share media and messages.

The reasons as to why people sext differs, it can be deliberate where the person sending the content means it to happen. It can also range from peer pressure or boosting self-esteem.

Risks of sexting

Out of your hands - The sender has no control about how it's passed on. It can mean that photos or videos end up being shared between adults they don't know.

Blackmail - An offender may threaten to share the pictures unless they receive money or more images.

Unwanted attention - grooming - Images posted online can attract the attention of sex offenders.

Emotional distress - It can lead to feeling embarrassed or humiliated. This can result in self-harming or in some cases suicide.

Bullying - If images are shared with their peers or in school, the child may be bullied.

The Law

According to **Section 1 of the Protection of Children Act 1978 and Section 160 Criminal Justice Act 1988**, if you’re under 18 it is against the law for anyone to take or have a sexual photo of you - even if it’s a selfie.

You are breaking the law if you:

- take an explicit photo or video of yourself or a friend
- share an explicit image or video of a child, even if it’s shared between children of the same age
- possess, download or store an explicit image or video of a child, even if the child gave their permission for it to be created

Sexting - How To Combat?

Think

Before sending an intimate photo, always remember to think. If the person asking for pictures acts up when you refuse - ask yourself:

- ***Is this someone you can trust?***
- ***If we break up, will this person respect me enough not to share my pictures?***

Other questions to think about before sending an image:

- ***How far will it reach?***
- ***Who might see it?***
- ***What are the risks?***
- ***What would my granny think if she saw the photo?***

Talk

- Have a conversation with the person you sent the image to. Ask them to delete it. The quicker you're able to do this the better
- Talk to somebody you trust who could advise you, the sooner the better

Report

- If an indecent or nude pic of you or a friend has been posted online, you can contact the website, such as Facebook or YouTube, to have it removed
- Report to the Internet Watch Foundation (IWF) who will contact the website to try and remove it without anyone else being involved.
- Child Exploitation and Online Protection Centre (CEOP) - **https://www.ceop.police.uk/Ceop-Report/**

A study by the Internet Watch Foundation showed that up to 88% of self-generated images have been collected and put onto other sites

Online Bullying

Online bullying is using social media, email, online games or any digital technology to threaten, tease, upset or humiliate someone else. It can happen anytime or anywhere, so it can feel like there's no escape. The 24/7 nature of online activity means you can be in contact at any time.

What should I do if I'm being bullied?

- ✔ Tell someone you trust, like a parent, teacher, family member, friend
- ✔ Save or print all messages from a bully for the purpose of documenting behaviour and future evidence
- ✔ Report - Most social networks will allow you to report offensive material. After taking a screenshot, you should report it to the service provider
- ✔ Block - The easiest way to stop someone bothering you online is to block their account from contacting you
- ✔ Do not retaliate or respond to abusive messages

Bullying vs Cyberbullying

Bullying	Cyberbullying
Face - to - face	24 hours a day, 7 days a week, 365 days a year
Can find a safe place or escape	No safe space - hard to escape
Limited to onlookers	Shared by a wide audience - can go viral in a matter of seconds
Bully can be identified	Bully can be anonymous
Can see facial and body reaction of target and onlookers	Harder to empathise with the target
	No geographical limitations
	The target can easily become the bully

1 in 3 children have been a victim of cyberbullying
McAfee survey of children and parents, 2014

Pathways into Cyber Crime

Hacking and Online Gaming - The Link

Suspects of hacking are getting younger, 17 is the average age according to the National Cyber Crime Unit, but some are as young as 12.

Readily available hacking tools and step by step tutorials are openly advertised on low level hacking or gaming forums. This means entry into cyber criminality is easier than ever as the skill barrier is lowered and hacking is simplified.

These circumstances have created an environment in which more young people are becoming involved in cyber crime.

Most often it starts with online gaming. Many start by getting involved with gaming cheats that talk about ways to change/"mod" games or even by launching a cyber-attack on an opponent to win a computer game.

This may seem innocent at first, but it can lead to being one of the gateways into cyber criminality. Individuals may use this as a ‘stepping stone’ to commit more serious offences like launching attacks on schools or even to a government agency they don't like.

Motivations

A report by the National Crime Agency (NCA, 2017) indicates that motivations can differ. Below are some of the explanations:

- **Sense of belonging** - through hacking forums and online communities
- **Proving** - a desire to prove oneself to the group
- **Improve** - a desire to improve one’s skills
- **Political** - use of skills to further political ends
- **Challenge** - to overcome an interesting challenge
- **Financial** - financial gain is often not a primary motivator

61% of hackers begin hacking before age 16
Hackers’ Profiling Project, UNICRI - 2012

Pathways into Cyber Crime

Hacking and Online Gaming - From the Offenders Mouth

"I was driven by my curiosity, I wanted to understand the best modifications and cheats … sharing this knowledge gave me credibility and popularity … the more my reputation increased, the more I felt I could interact with the smarter members … it was more interesting than working for a company, it gave me a feeling of power"

Subject 1 - Sold DDOS tools and botnets services - (NCA, 2017)

Consequences

There were many Subjects in the study by the National Crime Agency (NCA). The majority were jailed for a number of years for crimes falling under the Computer Misuse Act 1990.

It is important to understand that cybercrime is a serious criminal offence. The Police will make every effort to prosecute and arrest offenders. Punishment can range from fines / penalties, prevention of access to the internet and life imprisonment for more serious offences.

Using Your Talent

Channel your talent in IT into something positive and use your skills for good practice.

There are a number of organisations to help you develop your cyber skills:

- **Cyber Security Challenge** - a series of national competitions designed to test your cyber security skills
- **GCHQ Careers** - search for jobs within the tech industry that match your skills. GCHQ staff also provide an insight about what certain job profiles and roles entail
- **UKIE (UK Interactive Entertainment)** - involves the **Video Game Ambassadors** scheme where you can learn what it is like to become a game developer and how to get a job in the gaming industry
- **Cyber Retraining Academy** - offers skilled users a platform for training, apprenticeships and roles

Skills in coding, gaming, computer programming and cyber security are in high demand. There are many careers and opportunities available to anyone with an interest.

Employment in this field can provide a good salary from the start and offers attractive benefit packages. For example a senior cyber security consultant can earn between £80-90,000.

Subject 8 (NCA, 2017) claims that coding and programming educational opportunities or scholarships would have helped him by providing an outlet for his skills and interest.

Smartphone and Tablet Safety

Unlike a desktop computer where you are restricted to being in one place, smartphones and tablets allow you to carry out your online tasks anywhere you want.

The increased use of smartphones and tablets have aided our convenience but at the same time have generated a risk. In doing so, it has attracted interest of criminals who want to hack your devices for your personal and sensitive data. This is predominantly used for fraud purposes.

It is therefore imperative to take precautions to reduce the likelihood of this occurring.

Tips to help keep your device safe

Installing apps

Prevent app installs from unknown sources. On some devices you can change your settings that only allows app installations from acknowledged sources.

17% of all Android apps (nearly one million) are actually malware in disguise
Symantec's Internet Security Threat Report - 2015

Set PINS and passwords

Set up a PIN, password or swipe pattern on your home screen to protect your phone against unauthorised use.

Automatic login

Turn off setting which automatically saves the login details for your accounts. Although convenient, it does give criminals easy access to your online accounts if device is stolen.

Updates

Keep up to date with updates. As well as adding new features, updates will fix bugs or faults that make your device vulnerable.

Scams

Be mindful of scams that may install viruses or get you to share your personal information. They can come in the form of emails, SMS or MMS.

Antivirus

People generally don't think of their smartphones and tablets as PCs or laptops. Many may therefore disregard or 'not know' if an antivirus software is required. Antivirus will help to protect your device against viruses, malware and blocking dangerous links. It can be found on your device's app store or widely available at reputable retailers.

Glossary

Cookie
A small file which asks permission to be placed on your computer's hard drive. Cookies allow web applications to personalise your experience by gathering and remembering information about your preferences.

Encryption
The process of converting data into cipher text (a type of code) to prevent it from being understood by an unauthorised party.

.exe file
Executable file: used by programs to install and run on computers. Exercise caution if you receive an email with an executable file that you are not expecting, it could install a virus or malicious code which infects or locks your computer.

Firewall
Hardware or software designed to prevent unauthorised access to a computer or network over the internet.

Hacker
A hacker is a person who violates computer security for malicious reasons or for personal gain.

Pop-up
A small window which appears over a web page, usually to display an advertisement. Be wary of clicking on them, may infect your computer with viruses.

Two factor authentication
A method of obtaining additional evidence of identity to simply using passwords - such as a bank card.

Wireless hotspot
A publicly accessible wireless internet connection.

For a more in depth glossary, please visit **www.getsafeonline.org/jargon-buster/**

More Advice Online

There are a number of websites out there that offer lots of advice and guidance on how to stay safe online. Below are some useful links:

West Yorkshire Police - Cyber Unit
https://www.westyorkshire.police.uk/cyber

Action Fraud - Report fraud and Cyber Crime
http://www.actionfraud.police.uk/

The Internet Watch Foundation
https://www.iwf.org.uk/

The Child Exploitation and Online Protection (CEOP)
https://www.ceop.police.uk/Ceop-Report/

NSPCC - Keeping children safe online
https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety

Internet Matters - Help keeping children safe online
https://www.internetmatters.org/

Get Safe Online - Free online security advice
https://www.getsafeonline.org

ThinkUKnow - Guide to online safety
https://www.thinkuknow.co.uk/

UK Safer Internet Centre - For tips, advice and resources
https://www.saferinternet.org.uk/

Samaritans - Provides support and advice on a range of issues
https://www.samaritans.org/

Contact

To speak to us call **101** or in an emergency dial **999**

Online fraud can be reported to **Action Fraud** on **0300 123 2040** or online on **http://www.actionfraud.police.uk/contact-us**

Office of the
Police & Crime
Commissioner
West Yorkshire

WEST YORKSHIRE
POLICE